Symantec AntiVirus™ Scan Engine Software Developer's Guide

Symantec AntiVirus™ Scan Engine Software Developer's Guide

Documentation version 4.0

Copyright Notice

Trademarks

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC SOFTWARE LICENSE AGREEMENT
ENTERPRISE ANTIVIRUS SOFTWARE

THIS LICENSE AGREEMENT SUPERSEDES THE LICENSE AGREEMENT CONTAINED IN THE SOFTWARE INSTALLATION AND DOCUMENTATION.

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE" OR "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. LICENSE:

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the quantity of the Software for which You have paid the applicable license fees after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of licensed copies of this Software are as follows:

YOU MAY:

A. use the Software in the manner described in the Software documentation and in accordance with the License Module. If the Software is part of an offering containing multiple Software titles, the aggregate number of copies You may use may not exceed the aggregate number of licenses indicated in the License Module, as calculated by any combination of licensed Software titles in such offering. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single machine;

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

C. use the Software on a network or to protect a network such as at the gateway or on a mail server, provided that You have a license to the Software for each computer that can access the network;

D. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license; and

E. use the Software in accordance with any additional permitted uses set forth in Section 8 below.

YOU MAY NOT:

A. copy the printed documentation which accompanies the Software;

B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module;

F. use the Software in any manner not authorized by this license; nor

G. use the Software in any manner that contradicts any additional restrictions set forth in Section 8 below.

2. CONTENT UPDATES:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; some firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which You have purchased upgrade insurance for the product, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit You to obtain and use Content Updates.

3. LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. DISCLAIMER OF DAMAGES:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT

OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether You accept the Software.

5. U.S. GOVERNMENT RESTRICTED RIGHTS:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. EXPORT REGULATION:

Export or re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries Export or re-export of Software to any entity on the Denied Parties List and other lists promulgated by various agencies of the United States Federal Government is strictly prohibited.

7. GENERAL:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. The original of this Agreement has been written in English and English is the governing language of this Agreement. This Agreement may only be modified by a License Module which accompanies this license or by a written document which has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A. or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

8. ADDITIONAL RESTRICTIONS FOR SPECIFIED SOFTWARE:

A. If the Software You have licensed is a specified Symantec AntiVirus™ for a third-party product or platform, You may only use that specified Software with the corresponding product or platform. You may not allow any computer to access the Software other than a computer using the specified product or platform. In the event that You wish to use the Software with a certain product or platform for which there is no specified Software, You may use the Symantec AntiVirus Scan Engine.

B. If the Software you have licensed is Symantec AntiVirus for NetApp® Filer, the following additional use(s) and restriction(s) apply:

i) You may use the Software only with a NetApp Filer server;

ii) You may use the Software only with files accessed through a NetApp Filer; and

iii) You may not use the Software on a server that exceeds the specified capacity set forth in Your License Module.

C. If the Software you have licensed is Symantec AntiVirus for Web Servers, the following additional use(s) and restriction(s) apply:

i) You may use the Software only with files that are received from third parties through a Web server;

ii) You may use the Software only with files received from less than 10,000 unique third parties per month; and

iii) You may not charge or assess a fee for use of the Software for Your internal business.

D. If the Software You have licensed is Symantec Web Security, independent of version or operating platform designation, upon the expiration of Your right to acquire Content Updates, the filtering definitions corresponding with all previous Content Updates will be entirely deleted and will no longer be available for use with the Software. Upon the expiration of Your right to acquire Content Updates, access to updated virus definitions will no longer be available. However, You may continue to use virus definitions previously acquired.

E. If the Software You have licensed is Symantec AntiVirus Corporate Edition, You may not use the Software on or with devices on Your network running embedded operating systems specifically supporting network-attached storage functionality without separately licensing a version of such Software specifically licensed for a specific type of network-attached storage device under a License Module.

F. If the Software You have licensed is Symantec AntiVirus for EMC® Celerra™ File Server, You may use the Software only with EMC Celerra servers and only if You have a license to the Software for each Celerra AntiVirus Agent (CAVA) associated with each such server. You may not allow any computer to access the Software other than an EMC Celerra server.

Contents

Chapter 1

Getting started

This chapter includes the following topics:

About the Symantec AntiVirus Scan Engine

The Symantec AntiVirus Scan Engine, formerly marketed as CarrierScan Server, is a carrier-class virus scanning and repair engine. The Symantec AntiVirus Scan Engine features all of the key virus-scanning technologies available in the complete line of Symantec antivirus products, making the Symantec AntiVirus Scan Engine one of the most effective virus solutions available for detecting and preventing virus attacks.

The Symantec AntiVirus Scan Engine provides virus scanning and repair capabilities to any application on an IP network, regardless of platform, using one of several supported protocols. Any application can pass files to the Symantec AntiVirus Scan Engine for scanning, which in turn scans the files for viruses and returns a cleaned file if necessary.

For more information about supported virus detection technologies and virus protection, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

About licensing

Key features for the Symantec AntiVirus Scan Engine, including antivirus scanning and virus definitions updates, are activated by license. Licenses are initially installed after product installations through the Symantec AntiVirus Scan Engine administrative interface. When a license expires (for example, when a virus definitions product update subscription expires), a new license must be installed to renew the subscription. When no license is installed, functionality is limited. A license affects the relevant behavior only. For example, when no antivirus scanning license is installed, an administrator can access the administrative interface to view and modify settings and run reports, but no antivirus scanning is performed. When no virus definitions update license is installed, new virus definitions updates are not downloaded to keep protection current.

For more information about licensing, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

Integrating with the Symantec AntiVirus Scan Engine

Software developers can create client applications (or connectors) that let third-party applications integrate with the Symantec AntiVirus Scan Engine for virus scanning and repair services. Client applications can communicate with the Symantec AntiVirus Scan Engine using one of several supported protocols. However, only the native protocol and draft standard Internet Content Adaptation Protocol (ICAP) 1.0 are supported in the software developer's kit.

The Symantec AntiVirus Scan Engine also supports the ICAP 0.95 and Remote Procedure Call (RPC) 1.0 and 1.1 for NetApp Filer. These protocols are proprietary implementations and are not documented by Symantec.

About the native protocol

In its default configuration, the Symantec AntiVirus Scan Engine implements a simple TCP/IP protocol to provide antivirus functionality to client applications. This protocol is text-based, like HTTP or SMTP, and uses standard ASCII commands and responses to communicate between client and server.

To submit a file for scanning, a client connects to the specified IP port (for example, the default port 7777) and sends the file. After the client receives the scan results, the client and server disconnect. A new connection must be initiated to scan subsequent files.

Use the client-side application program interface (API) C library to configure an application to pass files to the Symantec AntiVirus Scan Engine for scanning using the native protocol. The API library consists of 10 functions that provide scan and repair services to client applications. The Symantec AntiVirus Scan Engine C API is available for Red Hat Linux 7.2 and later (using gcc 2.9x), Solaris 7 and later (using either gcc 2.9x or the Solaris C compiler), and Windows 2000 Server/Advanced Server (using Microsoft Visual C++). The provided C header file is included, and six function calls are used to process a file.

See "Configuring the Symantec AntiVirus Scan Engine for custom integrations" on page 15 and "Configuring clients using the client API library" on page 27.

For reference or debugging information about the native protocol, see "Native protocol reference" on page 71.

To develop a custom implementation that communicates directly with the Symantec AntiVirus Scan Engine, use ICAP.

See "Configuring clients using ICAP 1.0" on page 53.

About ICAP

ICAP is a lightweight protocol for executing a remote procedure call on HTTP messages. ICAP is part of an evolving architecture that lets corporations, carriers, and Internet service providers (ISPs) dynamically scan, change, and augment Web content as it flows through ICAP servers. The protocol lets ICAP clients pass HTTP messages to ICAP servers for *adaptation* (some sort of transformation or other processing, such as virus scanning). The server executes its transformation service on messages and responds to the client, usually with modified messages. The adapted messages may be either HTTP requests or HTTP responses.

In a typical integration, a caching proxy server retrieves the requested information from the Web. At the same time, it *caches* (stores a copy on disk) the information and, where possible, serves multiple requests for the same Web content from the cache. A caching proxy server can use ICAP to communicate with the Symantec AntiVirus Scan Engine and request that content that is retrieved from the Web be scanned and repaired.

The Symantec AntiVirus Scan Engine supports both the proprietary 0.95 and draft standard 1.0 implementations of ICAP. When you select ICAP as the communication protocol, the scan engine determines the appropriate version of ICAP to use based on the header data that is passed in from the client application. Instructions are provided for customizing applications using the ICAP 1.0 draft standard only.

See "Configuring clients using ICAP 1.0" on page 53.

Where to start

Complete the following steps to configure client applications to use either the Symantec AntiVirus Scan Engine native protocol or ICAP 1.0 to pass files to the scan engine for scanning.

- Become familiar with the design and features of the software.
  In addition to this guide, see the *Symantec AntiVirus Scan Engine Implementation Guide*.
- Decide how to deploy the Symantec AntiVirus Scan Engine on your network to meet your specific requirements.
  See "Considerations for implementation" on page 13.
- Install and configure the Symantec AntiVirus Scan Engine appropriately to use the native protocol or ICAP.
  See the *Symantec AntiVirus Scan Engine Implementation Guide*.

- If you are using the native protocol, install the API libraries.
  This guide provides the necessary information.
- Configure the client applications that will send files to the Symantec AntiVirus Scan Engine for scanning.
  This guide provides the necessary information.

Considerations for implementation

The Symantec AntiVirus Scan Engine can be easily implemented into an existing infrastructure. The Symantec AntiVirus Scan Engine runs on Solaris, Red Hat Linux, and Windows 2000 Server/Advanced Server platforms.

About Symantec AntiVirus Scan Engine deployment

In a typical configuration, files are passed to the Symantec AntiVirus Scan Engine via a socket over the network because the scan engine is running on a separate computer. Depending on the network setup, client applications (applications that have been configured to pass files to the scan engine for scanning) can pass a full path rather than the actual file to the Symantec AntiVirus Scan Engine. For example, files to be scanned may be located on a drive that can be mounted over the network, such as a shared drive in Windows or a network file system (NFS) drive. If the client application and the scan engine have access to a shared directory, the client application can place the file in the shared directory and pass the full path to the Symantec AntiVirus Scan Engine, which can access the file directly.

For cases in which the client application is running on the same computer as the Symantec AntiVirus Scan Engine, the client application can pass the file name to the scan engine, and the scan engine can open the file and scan it in place on the computer.

About automatic load balancing

If you are using the native protocol, the Symantec AntiVirus Scan Engine API provides scheduling across any number of computers that are running the Symantec AntiVirus Scan Engine. Client applications that pass files to the scan engine benefit from load-balanced virus scanning without any additional effort. The API determines the appropriate Symantec AntiVirus Scan Engine (when multiple scan engines are used) to receive the next file to be scanned, based on the scheduling algorithm.

If a Symantec AntiVirus Scan Engine is unreachable or goes down during a scan, another scan engine is called and the faulty scan engine is taken out of rotation for a period of time. If all of the scan engines are out of rotation, the faulty scan engines are called again. The API does not stop trying to contact the scan engine unless five engines are not functioning or it appears that a file that is being scanned might have caused more than one engine to go down.

For ICAP custom implementations, the integrator is responsible for load balancing. The Symantec AntiVirus Scan Engine does not provide an ICAP API for automatic load balancing.

Chapter 2

Configuring the Symantec AntiVirus Scan Engine for custom integrations

This chapter includes the following topics:

Considerations for custom integration

The Symantec AntiVirus Scan Engine is designed to be easily integrated into any environment to provide antivirus scanning for any application. Client applications are configured to pass files to the Symantec AntiVirus Scan Engine, which scans the files for viruses and returns cleaned files if necessary.

The Symantec AntiVirus Scan Engine also supports custom integrations, in which a software developer creates a client application (or connector) that provides virus scanning and repair services to a third-party application. The client application can communicate with the Symantec AntiVirus Scan Engine using either the native protocol or ICAP 1.0.

The Symantec AntiVirus Scan Engine must be configured to support the custom integration. This includes selecting the protocol, configuring protocol-specific options, and selecting the types of files to scan. Depending on the protocol that is used, the Symantec AntiVirus Scan Engine can be configured to scan only certain file types that are passed to it by client applications. In other cases, the client application must decide what to scan and what to do with the results. The client application must also be configured to communicate with the Symantec AntiVirus Scan Engine.

See "Configuring clients using the client API library" on page 27 or "Configuring clients using ICAP 1.0" on page 53.

Configuring the scan engine to use the native protocol

In its default configuration, the Symantec AntiVirus Scan Engine implements a simple TCP/IP protocol to provide antivirus functionality to client applications. This protocol is text-based like HTTP or SMTP, and uses standard ASCII commands and responses to communicate between client and server. To submit a file for scanning, a client connects to the specified IP port, sends the file to be scanned, and reads the results of the scan. After the scan results are received, the connection is terminated. A new connection is initiated for each file to be scanned.

If you select the native protocol, you must configure several protocol-specific options. Table 2-1 details the information that must be provided. For more information about installation and configuration, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

Table 2-1 Protocol-specific options for the native protocol

Option	Description
Scan engine bind address	By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by typing the appropriate bind address. You can use 127.0.0.1 (the loopback interface) to let only clients that are running on the same computer connect to the Symantec AntiVirus Scan Engine.
Port number	The specified port number must be exclusive to the Symantec AntiVirus Scan Engine. The default port number is 7777. If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service. If you are installing more than one instance of the Symantec AntiVirus Scan Engine on a single computer, each scan engine service must have a unique port number.
Local scan directory	You only need to provide a local scan directory when you are using local file scanning options (that is, the client application and the Symantec AntiVirus Scan Engine are running on the same computer and files are scanned in place on the computer) and you want to limit the Symantec AntiVirus Scan Engine so that only files under a particular directory can be scanned. If a local scan directory is not specified (which is the default), any file can be scanned. The directory that you specify must already exist.

If you are running the Symantec AntiVirus Scan Engine on Windows 2000 Server/Advanced Server and you change the protocol setting to the native protocol, you may need to change the service startup properties to identify an account that has sufficient permissions on which the Symantec AntiVirus Scan Engine will run.

See "Editing the service startup properties" on page 22.

To configure the native protocol

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Protocol tab, click **Native protocol**.
   The configuration settings display for the selected protocol.
3. In the Scan Engine bind address box, type a bind address, if necessary.
   By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by typing the appropriate bind address. Use 127.0.0.1 (the loopback interface) to let only clients that are running on the same computer connect to the Symantec AntiVirus Scan Engine.
4. In the Port number box, type the TCP/IP port number to be used by client applications to pass files to the scan engine for scanning.
   The default setting is port 7777.
5. In the Local scan directory box, type a local scan directory, if necessary.
   Any file can be scanned by default (if no local scan directory is specified). If you specify a directory for local scanning and you have client antivirus software installed to protect the computer that is running the Symantec AntiVirus Scan Engine, you must exclude the local scan directory from real-time scanning and from all scheduled and manually invoked scans by the client antivirus software before passing files to the Symantec AntiVirus Scan Engine for scanning.
6. Click **Confirm Changes** to save the configuration.
7. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
   - Click **Restart** to save your changes and restart the scan engine service now.
   - Click **Save/No Restart** to save your changes. (Changes will not take effect until the service is restarted.)

Configuring the scan engine to use ICAP

The Symantec AntiVirus Scan Engine can be configured to use ICAP to communicate with clients that are running either the proprietary version 0.95 or the draft standard version 1.0 of ICAP. Any appropriate client can use ICAP to

communicate with the Symantec AntiVirus Scan Engine to request the scanning and repairing of files.

You can configure multiple client applications that use different versions of ICAP to pass files to a single Symantec AntiVirus Scan Engine. When you select ICAP as the communication protocol for the scan engine, the scan engine determines the appropriate version of ICAP to use based on the header data that is passed in from the client application.

If you select ICAP as the protocol to be used by the Symantec AntiVirus Scan Engine, you must configure several ICAP-specific options. You must also configure the ICAP client to work with the Symantec AntiVirus Scan Engine. Table 2-2 details the information that must be provided.

Table 2-2 Protocol-specific options for ICAP

Option	Description
Scan Engine bind address	By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by entering the appropriate bind address. You can use 127.0.0.1 (the loopback interface) to let only clients that are running on the same computer connect to the Symantec AntiVirus Scan Engine.
Port number	The port number must be exclusive to the Symantec AntiVirus Scan Engine. The default port number is 1344. If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service. If you are installing more than one instance of the Symantec AntiVirus Scan Engine on a single computer, each scan engine service must have a unique port number.
HTML message displayed for infected files	The Symantec AntiVirus Scan Engine includes a default HTML message to display to users when access to a file is denied because it contains a virus. You can customize this message by specifying an alternate path and file name or by editing the existing file. If you choose to edit the existing file, you do not have to change this setting.
ICAP scan policy	When an infected file is found, the Symantec AntiVirus Scan Engine can do any of the following: ■ Scan only: Deny access to the infected file (but do nothing to the infected file). ■ Scan and delete: Delete all infected files, including files that are embedded in archive files, without attempting repair. ■ Scan and repair files: Attempt to repair infected files (but do nothing to files that cannot be repaired). ■ Scan and repair or delete: Attempt to repair infected files, and delete any unrepairable files from archive files.

To configure ICAP

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Protocol tab, click **ICAP**.
   The configuration settings display for the selected protocol.
3. In the Scan Engine bind address box, type a bind address, if necessary.
   By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by typing the appropriate bind address. Use 127.0.0.1 (the loopback interface) to let only clients that are running on the same computer connect to the Symantec AntiVirus Scan Engine.
4. In the Port number box, type the TCP/IP port number to be used by client applications to pass files to the Symantec AntiVirus Scan Engine for scanning.
   The default setting for ICAP is port 1344.
5. In the HTML message displayed for infected files box, type the path and file name to supply an alternate HTML file, if necessary.
6. In the ICAP scan policy drop-down list, select how you want the Symantec AntiVirus Scan Engine to handle infected files.
   The default setting is Scan and repair or delete.
7. Click **Confirm Changes** to save the configuration.
8. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes. (Changes will not take effect until the service is restarted.)

Changing an ICAP response

In its default configuration, the Symantec AntiVirus Scan Engine sends a 200 OK response for the following scenarios:

- No virus was detected during the scan.
- A virus was detected, but the file could not be repaired.
- A virus was detected and the Symantec AntiVirus Scan Engine is configured for scan only mode.

If a virus is detected and the file cannot be repaired, the Symantec AntiVirus Scan Engine includes a *replacement file* (the file specified for ICAPInfectionHTMLfile) in the body of the response message. The replacement file contains an HTML and/or email message that informs users that their access to a file is being denied because it contains a virus.

The Symantec AntiVirus Scan Engine default behavior deviates from the ICAP 1.0 draft standard, which does not support the automatic sending of a replacement file. In the ICAP 1.0 draft standard, this type of context-sensitive behavior is performed by the client rather than the scan engine.

The ICAP 1.0 draft standard also differs from the ICAP 0.95 implementation in this regard. If you were using ICAP 0.95 and want to maintain similar functionality when you migrate to ICAP 1.0, you should use the Symantec AntiVirus Scan Engine default ICAP response setting if the client application can support it.

If your client application closely follows the ICAP 1.0 draft standard, you might need to change the Symantec AntiVirus Scan Engine default ICAP response setting to receive an ICAP 403 response instead of a replacement file. The scan engine sends a 403 response if the file is infected and cannot be repaired. If no virus is detected, the scan engine returns a 200 OK response. You should change the default ICAP response setting only if you are sure that the client application supports this behavior.

Note: Most of the configuration options for the Symantec AntiVirus Scan Engine can be configured through the Web-based administrative interface. Under regular circumstances, you should not need to edit the configuration file.

To edit the Symantec AntiVirus Scan Engine configuration file

1. Locate the Symantec AntiVirus Scan Engine configuration file.
   The configuration file is located in the following default directories:
   - On Solaris and Linux: /opt/SYMCScan/etc/symcscan.cfg
   - On Windows 2000 Server/Advanced Server: C:\Program Files\Symantec\Scan Engine\symcscan.cfg

   If you are running more than one copy of the Symantec AntiVirus Scan Engine on a computer, make sure that you have the appropriate configuration file.
2. Open the configuration file with a text editor.
3. At ICAPResponse=, type one of the following to specify the scan engine response when a file is blocked because it is unrepairable (ICAP 1.0 only):
   - 0: Send an ICAP 403 response.
   - 1: Send a replacement file.
     This is the default setting.
4. Save the file.
5. Stop and restart the Symantec AntiVirus Scan Engine.

Editing the service startup properties

If the Symantec AntiVirus Scan Engine is installed on Windows 2000 Server/ Advanced Server and you change the protocol setting to the native protocol through the administrative interface, you may need to change the service startup properties to identify an account that has the appropriate permissions. The selected account must provide the Symantec AntiVirus Scan Engine with access and appropriate permissions to any shared drives or UNC paths for which scanning services are to be provided. This account should have access to any shared drives or UNC paths for which scanning is to be provided and should have Change permission if infected files that cannot be repaired are to be deleted.

To edit the service startup properties for Windows 2000 Server/Advanced Server

1. In the Windows 2000 Control Panel, click **Administrative Tools**.
2. Click **Services**.

   Two Symantec AntiVirus Scan Engine services are listed: Symantec AntiVirus Scan Engine Watchdog, which monitors the Symantec AntiVirus Scan Engine to ensure that it is always running, and Symantec AntiVirus Scan Engine.
3. Right-click **Symantec AntiVirus Scan Engine**, then click **Properties**.
4. In the Properties dialog box, on the Log On tab, click **This Account**.
5. Type the account name and password for the account on which the Symantec AntiVirus Scan Engine will run.

   Use the following format for the account name:

   domain\username
6. Click **OK**.
7. Stop and restart the Symantec AntiVirus Scan Engine service.

Specifying file types to scan

You can control which file types are scanned by specifying extensions that you do not want to scan (using an exclusion list) or by specifying extensions that you want to scan (using an inclusion list), or you can scan all file types regardless of extension. Inclusion and exclusion lists by definition do not scan all file types; thus, new types of viruses may not always be detected. Scanning all files regardless of extension is the most secure setting, but imposes the heaviest demand on resources.

Note: During virus outbreaks, you may want to scan all files even if you normally control the file types that are scanned with the inclusion or exclusion list.

The Symantec AntiVirus Scan Engine is configured by default to scan all files except those with the extensions listed in a prepopulated exclusion list. The default exclusion list contains those file types that are unlikely to contain viruses, but you can edit this list.

Using an inclusion list to control which types of files are scanned is the least secure setting. Only those files types that are specifically listed in an inclusion list are scanned; thus, with an inclusion list, there is an almost limitless number of

possible file extensions that are not scanned. For this reason, the inclusion list is not prepopulated, but you can choose to populate this list if you want to limit the file types that are scanned using an inclusion list.

If you use either the inclusion or the exclusion list to control the file types that are scanned (rather than scanning all files), the manner in which the list is applied differs depending on which of the following protocols are in use by the Symantec AntiVirus Scan Engine:

- Native protocol and ICAP 1.0: The inclusion or exclusion list is used by the Symantec AntiVirus Scan Engine only to determine which files to scan of those that are embedded in archival file formats (for example, .zip or .lzh files). All top level files that are sent to the Symantec AntiVirus Scan Engine are scanned regardless of file extension.

  Note: If you are using the native protocol or ICAP 1.0 and want to control the file types that are scanned at the top level, you must provide logic or take advantage of existing mechanisms on the client side to send only certain file types to the Symantec AntiVirus Scan Engine for scanning. The logic on the client side controls the types of files that are scanned at the top level, and the extension list setting controls which embedded files are scanned.

- ICAP 0.95: The inclusion or exclusion list applies to all files that are sent to the Symantec AntiVirus Scan Engine for scanning. This extension list is consulted for both top level files and embedded files that are contained in archival file formats (for example, .zip or .lzh files).

Specify which file types to scan

You can control which file types are scanned by specifying extensions that you want to scan or that you do not want to scan, or you can scan all files regardless of extension. The Symantec AntiVirus Scan Engine is configured by default to scan all files except those with extensions listed in the prepopulated exclusion list.

To scan all files regardless of extension

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, click **Scan all files regardless of extension**.
3. Click **Confirm Changes** to save the configuration.
4. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes. (Changes will not take effect until the service is restarted.)

To scan all files except for those with extensions that are in the exclusion list

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, click **Scan all files except those with the following extensions**.
3. Edit the extension list to add extensions that you do not want to scan or delete extensions that you want to scan.

   Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To exclude files with no extension, use two adjacent semicolons (for example, .com;.exe;;).
4. To restore the default extension lists, click **Restore default lists**.
5. Click **Confirm Changes** to save the configuration.
6. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes. (Changes will not take effect until the service is restarted.)

To scan only files with extensions that are in the inclusion list

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, check **Scan files with the following extensions**.
3. Edit the inclusion list to add extensions that you want to scan or delete extensions that you do not want to scan.

   Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To scan files that have no extensions, use two adjacent semicolons (for example, .com;.exe;;).
4. Click **Confirm Changes** to save the configuration.
5. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes. (Changes will not take effect until the service is restarted.)

Chapter 3

Configuring clients using the client API library

This chapter includes the following topics:

General procedure for scanning

The Symantec AntiVirus Scan Engine client API library provides a set of functions to simplify communication with the Symantec AntiVirus Scan Engine using the native protocol.

The procedure for scanning files is as follows:

- The client calls ScanClientStartUp() once to initialize the client library and to set up the scheduling.
- Files are scanned using either ScanClientScanFile() or ScanClientStreamStart(), ScanClientStreamSendBytes() (as many times as necessary), and ScanClientStreamFinish().
- Information on infections found (if any) is obtained using ScanResultGetNumProblems() and ScanResultGetProblem().
- Completion of scanning for a particular file is indicated using ScanResultsFree().
- Completion of all scanning is indicated (for example, before program termination) using ScanClientShutDown() to free resources.

Compiling and linking

Table 3-1 describes requirements for compiling and linking on Solaris, Linux, and Windows 2000 Server/Advanced Server.

Note: The Symantec AntiVirus Scan Engine API libraries are supported with gcc compiler version 2.9x only. A known compatibility issue exists with gcc version 3.x.

Table 3-1 Compiling and linking requirements

Platform	Include	Initialize	Link
Solaris	#include “symcsapi.h”	none	libsocket.a libnsl.a (for example, gcc -lsocket -lnsl)
Red Hat Linux	#include “symcsapi.h”	none	libnsl.a (for example, gcc -lnsl)
Windows NT/2000	#include “symcsapi.h”	initialize winsock	winsock (for example, WS2_32.LIB)

Windows 2000 Server/Advanced Server

The source code should #include the symcsapi.h file and link to SYMCSAPI.lib. The library should be compiled with multithreaded runtime libraries. For example, in Microsoft Visual Studio under Project Settings, click the C/C++ tab, click Code Generation, and click Multithreaded Libraries. You must link to the winsock library (WS2_32.LIB) and initialize winsock in the source code before scanning files. You must release winsock when all network access is complete (usually just before exiting the program).

Initializing winsock

The client application must initialize winsock before scanning files. The following example demonstrates winsock initialization:

```
#include <windows.h>
.
.
.
    // start up winsock
    WORD wVersionRequested;
    WSADATA wsaData;
    int err;


    // Load WinSock, request version 1.0.
    wVersionRequested = MAKEWORD(1, 0);
    err = WSAStartup(wVersionRequested, &wsaData);
    if (err != 0)
    {
        // ERROR
    }


    // Confirm WinSock supports the version we requested.
    if (LOBYTE(wsaData.wVersion) != 1 ||
            HIBYTE(wsaData.wVersion) != 0)
    {
        WSACleanup();
        // ERROR
    }
```

Shutting down winsock

You must release winsock when all network access is complete.

```
    if (WSACleanup() == SOCKET_ERROR)
        ;// ERROR
```

Solaris

The source code that makes calls to the library should #include the symcsapi.h header file. In the makefile (or command line) that compiles the program, libsymcsapi.a should be added and, if it is not already used, -lnsl -lsocket should be added. For example:

gcc mycode.c libsymcsapi.a -lsocket -lnsl

Red Hat Linux

The source code that makes calls to the library should #include the symcsapi.h header file. In the makefile (or command line) that compiles the program, libsymcsapi.a should be added and, if it is not already used, -lnsl should be added. For example:

gcc mycode.c libsymcsapi.a -lnsl

Exceptions and error handling

The Symantec AntiVirus Scan Engine C API library does not throw exceptions or include exception handling. Detected errors are returned as result codes from the functions.

API functions

The API functions are as follows:

- ScanClientStartUp
- ScanClientScanFile
- ScanResultGetNumProblems
- ScanResultGetProblem
- SC_DECODE_DISPOSITION
- ScanResultsFree
- ScanClientShutDown
- ScanClientStreamStart
- ScanClientStreamSendBytes
- ScanClientStreamFinish
- ScanClientStreamAbort

ScanClientStartUp

The ScanClientStartUp function lets a new client begin submitting files to the Symantec AntiVirus Scan Engine.

```
SC_ERROR ScanClientStartUp
(
    HSCANCLIENT     *client,
    LPSTR           pszClientConfiguration
)
```

ScanClientStartUp parameters

Table 3-2 lists the parameters that are used.

Table 3-2 ScanClientStartUp parameters

Parameter	Description
client	Address of an HSCANCLIENT variable. The HSCANCLIENT variable is a handle to a status data structure used throughout the scanning process. This variable contains information about the servers that are being used and the scheduling mechanism. Memory is allocated for this data structure by this call and must be freed using ScanClientShutDown() when scanning is completed.
pszClientConfiguration	A null terminated string that contains configuration information. Entries are separated with three semicolons (;;;), and no spaces are allowed. Two options are currently supported: ■ "Server:ipaddress:port;;;…" All Symantec AntiVirus Scan Engines that are used should be listed. At least one server must be listed. ■ "FailRetryTime:<seconds>" If the client fails to connect to a Symantec AntiVirus Scan Engine, wait <seconds> before trying to connect to that server again (use only the other servers in the meantime, unless they have all failed recently).

ScanClientStartUp return codes

Return codes are listed in Table 3-3. Negative values are warnings. Positive values are errors.

Table 3-3 ScanClientStartUp return codes

Return code	Description
SC_OUTOFRANGE_PARAMETER	At least one parameter that was passed to the function was out of range.
SC_FILEIO_ERROR	A file input/output error has occurred.
SC_MEMORY_ERROR	A memory allocation error has occurred.
SC_SOCKET_FAILURE	A socket communications error has occurred.
SC_INVALID_PARAMETER	A parameter that was passed to the function was invalid.
SC_OK	Success.
SC_NULL_PARAMETER	A parameter that was passed to the function is NULL when it shouldn't be.

ScanClientStartUp description

In a multithreaded environment, the client should make a single call to ScanClientStartUp on behalf of all of its threads. This way, all threads use scheduling via a single scheduler rather than multiple schedulers.

Parameter pszClientConfiguration should look like the following:

Server:1.2.3.4:7777;;;Server:1.2.3.5:7777

At least one Symantec AntiVirus Scan Engine must be specified. Entries are separated with three semicolons. No spaces are allowed. If the default port (7777) is used, the port number (and the colon) can be omitted.

ScanClientScanFile

The ScanClientScanFile function is called to have the Symantec AntiVirus Scan Engine scan a file for viruses.

Note: All file names must be Unicode UTF-8 encoded.

```
SCSCANFILE_RESULT ScanClientScanFile
(
    HSCANCLIENT    hScanClient,
    LPSTR          pszOriginalFileName,
    LPSTR          pszActualFileName,
    LPSTR          pszOutputFileName,
    LPSTR          pszScanPolicy,
    LPHSCANRESULTS phScanResults
)
```

ScanClientScanFile parameters

Table 3-4 lists the parameters that are used.

Table 3-4 ScanClientScanFile parameters

Parameter	Description
hScanClient	An HSCANCLIENT variable that has been initialized. See "ScanClientStartUp" on page 31.
pszOriginalFileName	The name of the file to be scanned. (The original name of the file on the end user's computer.) This parameter is ignored if the PassFileByName=1 string is set in pszScanPolicy.
pszActualFileName	The name (path) of the file to scan on the Scan Client computer. This path may or may not be different than pszOriginalFileName. For example, an end user may upload a file to be scanned called sample.doc, but the same file may be stored on the ISP computer as temp123.doc. In this case, the pszOriginalFileName is sample.doc, but the pszActualFileName may be /tmp/temp123.doc.

Table 3-4 ScanClientScanFile parameters

Parameter	Description
pszOutputFileName	The storage location for the repaired file. (No output file is created unless the input file is infected and the infection is repairable.) This parameter can be one of the following: ■ A null-terminated string that is a path to where the repaired file is to be stored. ■ A char array at least MAX_STRING long, with the first byte set to '\0'. The API generates a file name for the repair file. When the function returns, pszOutputFileName is set to the name of the repaired file. If this parameter is NULL, the API has the Symantec AntiVirus Scan Engine scan the file for viruses but not attempt repair. The Symantec AntiVirus Scan Engine ignores this parameter if local scanning options are set using pszScanPolicy.
pszScanPolicy	A null-terminated string of the form <option:value>;;;<option:value>… No spaces are allowed. The following options are supported: ■ ScanOnly:1: Scan for viruses but do not attempt repair. This option is the same as passing in NULL for pszOutputFileName. ■ AlwaysReportDefInfo:1: If a clean file is scanned, a Problem Incident is created with only the virus definitions date and revision number. ■ RepairOnly:1: Attempt to repair infected files but do not delete files that cannot be repaired. ■ PassFileByName:1: The file to be scanned is on the same computer as the Symantec AntiVirus Scan Engine or can be accessed via NFS or another network file protocol. In this case, the file is not sent over a socket. Instead, the Symantec AntiVirus Scan Engine opens the file directly for scanning. If a repair is required, the repair is made in the local directory. If this string is set, the Symantec AntiVirus Scan Engine uses the pszActualFileName parameter to read the file and uses the ExtensionList= and ExclusionList= options to determine how to handle scanning for a specific file type.

Table 3-4 ScanClientScanFile parameters

Parameter	Description
phScanResults	When the function returns, this handle points at a structure that contains information about any problems (infections) found during the scan. If none were found, this parameter is NULL unless the AlwaysReportDefInfo:1 policy is used in the scan. Information regarding problems is extracted using the described functions. If this parameter is not NULL, the memory must be released using ScanResultsFree().

ScanClientScanFile return codes

Return codes are listed in Table 3-5. Negative values indicate that a virus was detected. Positive values are errors. Zero indicates a clean file.

Table 3-5 ScanClientScanFile return codes

Return code	Description
SCSCANFILE_INF_NO_REP	The file was infected with a virus, but no repair was possible.
SCSCANFILE_INF_PARTIAL_REP	The file was infected, but only a partial repair was possible.
SCSCANFILE_INF_REPAIRED	The file was infected, and repair was successful.
SCSCANFILE_CLEAN	No virus was found.
SCSCANFILE_FAIL_CONNECT	Attempt to connect to a Symantec AntiVirus Scan Engine failed.
SCSCANFILE_FAIL_INPUTFILE	A problem was encountered reading the file to be scanned.
SCSCANFILE_FAIL_ABORTED	The scan was aborted abnormally.
SCSCANFILE_INVALID_PARAM	Function was called with an invalid parameter.
SCSCANFILE_FAIL_RECV_FILE	An error occurred when attempting to receive the repaired file.
SCSCANFILE_FAIL_MEMORY	A memory allocation error has occurred.

Table 3-5 ScanClientScanFile return codes

Return code	Description
SCSCANFILE_FAIL_FILE_ACCESS	The server couldn't access the file to be scanned. This error usually occurs for LOCAL scans when file permissions are wrong or when the file is not in the path that is specified in the LocalFileScanDir parameter on the server.
SCSCANFILE_FAIL_EXTRACTTIME	The file could not be scanned because the specified maximum amount of time that was spent decomposing a container file and its contents was exceeded.
SCSCANFILE_FAIL_EXTRACTDEPTH	The file could not be scanned because the specified maximum number of nested levels to be decomposed for scanning was exceeded.
SCSCANFILE_FAIL_EXTRACTSIZE	The file could not be scanned because the specified maximum file size for individual files in a container file was exceeded.
SCSCANFILE_FAIL_REPAIRFILE	An internal server error occurred while the scan engine was attempting to repair the file.
SCSCANFILE_ERROR_SCANNINGFILE	An internal server error occurred while the scan engine was attempting to scan the file.

ScanClientScanFile description

The ScanClientScanFile function determines the appropriate Symantec AntiVirus Scan Engine (when multiple Symantec AntiVirus Scan Engines are running) based on the scheduling algorithm. If a Symantec AntiVirus Scan Engine is unreachable or goes down during a scan, another server is called and the faulty server is taken out of rotation for a period of time. If all Symantec AntiVirus Scan Engines are out of rotation, the faulty servers are called again. The ScanClientScanFile function does not stop trying to contact a Symantec AntiVirus Scan Engine unless five servers are not functioning or it appears that a file being scanned might have caused two servers to go down.

ScanResultGetNumProblems

The ScanResultGetNumProblems function indicates the number of infections that are contained in an HSCANRESULT after scanning a file. Use the

ScanResultGetProblem() function to get information about the infections that are reported in an HSCANRESULT after scanning a file.

```
SC_ERROR ScanResultGetNumProblems
(
    HSCANRESULT hScanResult,
    int *nNumProblems
)
```

ScanResultGetNumProblems parameters

Table 3-6 lists the parameters that are used.

Table 3-6 ScanResultGetNumProblems parameters

Parameter	Description
hScanResult	An HSCANRESULT variable that is returned by ScanClientScanFile() or ScanClientStreamFinish().
nNumProblems	When the function returns, this parameter is set to the number of infections in the scanned file. If the AlwaysReportDefInfo:1 scan policy option is used, at least one (blank) incident is reported, along with the virus definitions date and revision number.

ScanResultGetNumProblems return codes

Return codes are listed in Table 3-7. Negative values are warnings. Positive values are errors.

Table 3-7 ScanResultGetNumProblems return codes

Return code	Description
SC_OUTOFRANGE_PARAMETER	At least one parameter that was passed to the function was out of range.
SC_FILEIO_ERROR	A file input/output error has occurred.
SC_MEMORY_ERROR	A memory allocation error has occurred.
SC_INVALID_PARAMETER	A parameter that was passed to the function was invalid.
SC_OK	Success.
SC_NULL_PARAMETER	A parameter that was passed to the function is NULL when it shouldn't be.

ScanResultGetProblem

The ScanResultGetProblem function is used to get specific information about a virus.

```
SC_ERROR ScanResultGetProblem
(
    HSCANRESULT hScanResult,
    int nProblemNum,
    int nAttribute,
    LPSTR pszValueOut,
    LPINT pnValueLengthInOut
)
```

ScanResultGetProblem parameters

Table 3-8 lists the parameters that are used.

Table 3-8 ScanResultGetProblem parameters

Parameter	Description
hScanResult	An HSCANRESULT variable that is returned by ScanClientScanFile() or ScanClientStreamFinish().
nProblemNum	Integer specifying which problem entry is being investigated.
nAttribute	Identifies which attribute is being queried. Valid attributes are: ■ SC_PROBLEM_FILENAME: The file name in which the infection occurred. ■ SC_PROBLEM_VIRUSNAME: The name of the virus that has infected the file. ■ SC_PROBLEM_VIRUSID: The unique numerical ID of the virus. ■ SC_PROBLEM_DISPOSITION: Problem resolution. This value is a number (in a string format) that indicates whether the virus was cleaned from the file. ■ SC_PROBLEM_DEFINITION_DATE: The date stamp on the virus definitions. ■ SC_PROBLEM_DEFINITION_REV: Revision number of the definitions.
pszValueOut	Buffer that holds the attribute value being retrieved.

Table 3-8 ScanResultGetProblem parameters

Parameter	Description
pnValueLengthInOut	Pointer to variable that holds the size of the pszValueOut buffer. When the function returns, the size of the attribute string is placed in this variable. You can determine if the buffer was large enough to hold the entire string by seeing whether pnValueLengthInOut is smaller after the call than before (if the value is smaller, the buffer was large enough).

ScanResultGetProblem return codes

Return codes are listed in Table 3-9. Negative values are warnings. Positive values are errors.

Table 3-9 ScanResultGetProblem return codes

Return code	Description
SC_OUTOFRANGE_PARAMETER	At least one parameter that was passed to the function was out of range.
SC_FILEIO_ERROR	A file input/output error has occurred.
SC_MEMORY_ERROR	A memory allocation error has occurred.
SC_INVALID_PARAMETER	A parameter that was passed to the function was invalid.
SC_OK	Success.
SC_NULL_PARAMETER	A parameter that was passed to the function is NULL when it shouldn't be.

ScanResultGetProblem description

A buffer is supplied to hold the information about the virus, and a pointer is supplied to an integer that holds the size of the buffer. When the function returns, the integer holds the amount of data that was placed in the buffer. If the buffer is not large enough to hold the information, as much information as possible is copied into the buffer. If the value of the integer is the same after the call as it was before the call, the buffer most likely was not large enough to hold the information. See description of the nAttribute parameter for the type of information that can be retrieved.

SC_DECODE_DISPOSITION

The problem disposition is retrieved with ScanResultGetProblem() in the form of a string. The SC_DECODE_DISPOSITION function is a macro that converts the string to an integer and defines the result codes as integers for easier processing.

```
int SC_DECODE_DISPOSITION( char *pszDisposition )
```

SC_DECODE_DISPOSITION parameters

Table 3-10 lists the parameters that are used.

Table 3-10 SC_DECODE_DISPOSITION parameters

Parameter	Description
pszDisposition	The pszValueOut that is returned from ScanResultGetProblem with nAttribute equal to SC_PROBLEM_DISPOSITION.

SC_DECODE_DISPOSITION return codes

Return codes are listed in Table 3-11.

Table 3-11 SC_DECODE_DISPOSITION return codes

Return code	Description
SC_DISP_REPAIRED	The infected file was repaired.
SC_DISP_UNREPAIRED	The infected file was not repaired.
SC_DISP_DELETED	The infected file was deleted.

ScanResultsFree

The ScanResultsFree function is used to free the HSCANRESULT structure. This function must be called when the result structure is no longer needed to free the allocated memory.

```
SC_ERROR ScanResultsFree( HSCANRESULT hScanResult )
```

ScanResultsFree return codes

Return codes are listed in Table 3-12. Negative values are warnings. Positive values are errors.

Table 3-12 ScanResultsFree return codes

Return code	Description
SC_MEMORY_ERROR	A memory allocation error has occurred.
SC_OK	Success.
SC_NULL_PARAMETER	A parameter that was passed to the function is NULL when it shouldn't be.

ScanClientShutDown

The ScanClientShutDown function is called to clean up after all scanning is complete (for example, before program termination).

```
SC_ERROR ScanClientShutDown( HSCANCLIENT hScanClient )
```

ScanClientShutDown return codes

Return codes are listed in Table 3-13. Negative values are warnings. Positive values are errors.

Table 3-13 ScanClientShutDown return codes

Return code	Description
SC_FILEIO_ERROR	A file input/output error has occurred.
SC_MEMORY_ERROR	A memory allocation error has occurred.
SC_SOCKET_FAILURE	A socket communications error has occurred.
SC_INVALID_PARAMETER	A parameter that was passed to the function was invalid.
SC_OK	Success.
SC_NULL_PARAMETER	A parameter that was passed to the function is NULL when it shouldn't be.

ScanClientStreamStart

The ScanClientStreamStart function is used for scanning streams. It can also be used when you want to accept an input stream for scanning rather than an entire file at one time. For example, if a file is being received via an HTTP stream as a user uploads a file to a Web site, stream scanning can be used.

Note: All file names must be Unicode UTF-8 encoded.

```
SC_ERROR ScanClientStreamStart
(
    HSCANCLIENT hScanClient,
    LPSTR       pszOriginalFileName,
    LPSTR       pszScanPolicy,
    HSCANSTREAM *phScanStream
)
```

ScanClientStreamStart parameters

Table 3-14 lists the parameters that are used.

Table 3-14 ScanClientStreamStart parameters

Parameter	Description
hScanClient	This parameter should be set up using ScanClientStartUp().
pszOriginalFileName	The original name of the file to be scanned as it was named on the end user's computer.
pszScanPolicy	A null-terminated string of the form <option:value>;;;<option:value>… No spaces are allowed. See "ScanClientScanFile" on page 33.
phScanStream	Pointer to an HSCANSTREAM variable.

ScanClientStreamStart return codes

Return codes are listed in Table 3-15. Negative values are warnings. Positive values are errors.

Table 3-15 ScanClientStreamStart return codes

Return code	Description
SC_OUTOFRANGE_PARAMETER	At least one parameter that was passed to the function was out of range.
SC_FILEIO_ERROR	A file input/output error has occurred.
SC_MEMORY_ERROR	A memory allocation error has occurred.
SC_SOCKET_FAILURE	A socket communications error has occurred.
SC_INVALID_PARAMETER	A parameter that was passed to the function was invalid.
SC_OK	Success.
SC_NULL_PARAMETER	A parameter that was passed to the function is NULL when it shouldn't be.

Setting up stream scanning

The stream scanning feature lets the stream from the end user's computer be sent directly to the Symantec AntiVirus Scan Engine, rather than first receiving the entire file and then calling ScanClientScanFile().

To set up stream scanning

1. Call ScanClientStreamStart() to initialize the HSCANSTREAM variable.

   ScanClientStreamStart() must be called for each file to be scanned to initialize the HSCANSTREAM variable. HSCANSTREAM variables can be reused only after the stream has been closed with ScanClientStreamFinish() or ScanClientStreamAbort(). All file names must be Unicode UTF-8 encoded.

2. Send data to the server in chunks as it is received using ScanClientStreamSendBytes().

3. When all data is sent, call ScanClientStreamFinish().

   To abort the scan between the …Start() and …Finish() calls, call ScanClientStreamAbort().

ScanClientStreamSendBytes

The ScanClientStreamSendBytes function is used to send chunks of data after HSCANSTREAM has been initialized with ScanClientStreamStart().

See "ScanClientStreamStart" on page 42.

```
SC_ERROR ScanClientStreamSendBytes
(
    HSCANSTREAM hStream,
    LPBYTE      lpabyData,
    DWORD       dwLength
)
```

ScanClientStreamSendBytes parameters

Table 3-16 lists the parameters that are used.

Table 3-16 ScanClientStreamSendBytes parameters

Parameter	Description
hStream	The HSCANSTREAM variable, which must be initialized by a call to ScanClientStreamStart().
lpabyData	Pointer to a buffer that contains the next chunk of data to be sent.
dwLength	Size, in bytes, of the next chunk of data to be sent.

ScanClientStreamSendBytes return codes

Return codes are listed in Table 3-17. Negative values are warnings. Positive values are errors.

Table 3-17 ScanClientStreamSendBytes return codes

Return code	Description
SC_OUTOFRANGE_PARAMETER	At least one parameter that was passed to the function was out of range.
SC_FILEIO_ERROR	A file input/output error has occurred.
SC_MEMORY_ERROR	A memory allocation error has occurred.
SC_SOCKET_FAILURE	A socket communications error has occurred.
SC_INVALID_PARAMETER	A parameter that was passed to the function was invalid.
SC_OK	Success.
SC_NULL_PARAMETER	A parameter that was passed to the function is NULL when it shouldn't be.

ScanClientStreamFinish

The ScanClientStreamFinish function must be called after an entire file has been sent to the Symantec AntiVirus Scan Engine to be scanned using ScanClientStreamSendBytes().

Note: All file names must be Unicode UTF-8 encoded.

See "ScanClientStreamStart" on page 42.

```
SCSCANFILE_RESULT ScanClientStreamFinish
(
    HSCANSTREAM    hStream,
    LPSTR          pszOutputFileName,
    LPHSCANRESULTS phScanResults
)
```

ScanClientStreamFinish parameters

Table 3-18 lists the parameters that are used.

Table 3-18 ScanClientStreamFinish parameters

Parameter	Description
hStream	The HSCANSTREAM variable, which must be initialized by a call to ScanClientStreamStart().
pszOutputFileName	The storage location for the repaired file. (No output file is created unless the input file is infected and the infection is repairable.) This parameter can be one of the following: ■ A null-terminated string that is a path to where the repaired file is to be stored. ■ A char array at least MAX_STRING long, with the first byte set to '\0'. The API generates a file name for the repair file. When the function returns, pszOutputFileName is set to the name of the repaired file. ■ If this parameter is NULL, the API has the Symantec AntiVirus Scan Engine scan the file for viruses but not attempt repair.
phScanResults	When the function returns, this handle points at a structure that contains information about any problems (infections) found during the scan. If none were found, this parameter is NULL unless the AlwaysReportDefInfo:1 policy is used in the scan. Information regarding problems is extracted using the described functions. If this parameter is not NULL, the memory must be released using ScanResultsFree().

ScanClientStreamFinish return codes

Return codes are listed in Table 3-19. Negative values are warnings. Positive values are errors.

Table 3-19 ScanClientStreamFinish return codes

Return code	Description
SC_FILEIO_ERROR	A file input/output error has occurred.
SC_MEMORY_ERROR	A memory allocation error has occurred.
SC_SOCKET_FAILURE	A socket communications error has occurred.

Table 3-19 ScanClientStreamFinish return codes

Return code	Description
SC_INVALID_PARAMETER	A parameter that was passed to the function was invalid.
SC_OK	Success.
SC_NULL_PARAMETER	A parameter that was passed to the function is NULL when it shouldn't be.

ScanClientStreamAbort

The ScanClientStreamAbort function is called to abort a scan between calls to ScanClientStreamStart() and ScanClientStreamFinish().

```
SC_ERROR ScanClientStreamAbort
(
    HSCANSTREAM hStream
)
```

ScanClientStreamAbort return codes

Return codes are listed in Table 3-20. Negative values are warnings. Positive values are errors.

Table 3-20 ScanClientStreamAbort return codes

Return code	Description
SC_OUTOFRANGE_PARAMETER	At least one parameter that was passed to the function was out of range.
SC_FILEIO_ERROR	A file input/output error has occurred.
SC_MEMORY_ERROR	A memory allocation error has occurred.
SC_SOCKET_FAILURE	A socket communications error has occurred.
SC_INVALID_PARAMETER	A parameter that was passed to the function was invalid.
SC_OK	Success.
SC_NULL_PARAMETER	A parameter that was passed to the function is NULL when it shouldn't be.

Sample code

The sample code shown in this manual is for convenience. Sample code also is included on the distribution CD. Sample code implements a command-line scanner that uses the Symantec AntiVirus Scan Engine for virus scanning.

This example demonstrates the use of the ScanClientScanFile() function. Note that all file names must be Unicode UTF-8 encoded.

On Solaris, compile the code using code similar to the following:

```
gcc apidemo.c libsymcsapi.a -lsocket -lnsl -o apidemo
```

On Windows, it must be linked to WS2_32.LIB.

```
#if defined( WIN32 )
#pragma warning(push,3)
#endif

#include <stdio.h>
#include <string>
#include "symcsapi.h"

#if defined( WIN32 )
#include <windows.h>
#endif

// Prototypes

void print_prob_info( HSCANRESULTS hResults, int iWhichProblem );

int scanfile( HSCANCLIENT scanclient, char *orig_name, char
*actual_name);

int main( int argc, char *argv[])
{

    HSCANCLIENT scanclient=NULL;
    char pszStartUpString[MAX_STRING];
    int i;

#if defined( WIN32 )

    // start up winsock
    WORD wVersionRequested;
    WSADATA wsaData;
    int err;
```

```
    // Load WinSock, request version 1.0.
    wVersionRequested = MAKEWORD(1, 0);
    err = WSAStartup(wVersionRequested, &wsaData);
    if (err != 0)
    {
        return 3;// ERROR
    }

    // Confirm WinSock supports the version we requested.
    if (LOBYTE(wsaData.wVersion) != 1 ||
            HIBYTE(wsaData.wVersion) != 0)
    {
        WSACleanup();
        return 3;// ERROR
    }

#endif // defined( WIN32 )

    if( argc < 3 )
    {
        printf( "Usage: %s <ipaddress>:<port> <input-
            file> [<input-file>...]\n", argv[0]);
        return 1;
    }

    sprintf( pszStartUpString, "server:%s", argv[1] );

    if( ScanClientStartUp( &scanclient, pszStartUpString) > 0 )
    {
        printf( "Error in ScanClientStartUp\n");
        return 1;
    }

    for( i=2; i<argc; i++ )
    {
        printf( "============================\n");
        printf( "Scanning file: %s\n", argv[i] );
        printf( "============================\n");
        scanfile( scanclient, argv[i], argv[i] );

    }

    ScanClientShutDown( scanclient );

#if defined( WIN32 )

    if (WSACleanup() == SOCKET_ERROR)
    {
        // ERROR
    }

#endif

    return 0;
}
```

```
int scanfile( HSCANCLIENT scanclient, char *orig_name, char
                *actual_name)
{
    HSCANRESULTS results=NULL;
    SCSCANFILE_RESULT answer;
    int i;
    char repair_file[MAX_STRING];
    int numproblems=0;

    // Set up the buffer to accept the repair filename
    repair_file[0] = 0;

    // Do the scan.
    answer = ScanClientScanFile( scanclient,
        orig_name,
        actual_name,
        repair_file,
        "",
        &results
        );

    if( answer > 0 )
    {
        printf( "**** ERROR! Couldn't scan file\n");
        return 1;
    }

    switch( answer )
    {
    case SCSCANFILE_INF_NO_REP:
        printf( "File is infected and cannot be repaired\n");
        break;
    case SCSCANFILE_INF_PARTIAL_REP:
        printf( "File is infected and was partially repaired\n");
        break;
    case SCSCANFILE_INF_REPAIRED:
        printf( "File was infected, and has been repaired\n");
        break;
    case SCSCANFILE_CLEAN:
        printf( "File is clean\n");
        break;
    default:
        printf("ScanClientScanFile returned an unexpected value\n");
        break;
    }

    // The results structure will be non-null if a
    //  virus was detected.
    if( results )
    {
        if( strlen( repair_file ) )
            printf( "Repaired file saved as: %s\n", repair_file );
        else
            printf( "No repair file generated\n");
```

```
        if( ScanResultGetNumProblems( results, &numproblems ) > 0 )
        {
            printf( "Error getting number of problems\n");
            return 2;
        }
        printf("%s had %d infection(s):\n", actual_name,
                numproblems );
    }
    else
        numproblems = 0;

    for( i=0; i<numproblems; i++ )
    {
        print_prob_info( results, i );
    }

    // Be sure to free the results when done!
    ScanResultsFree( results );

    return 1;
}


void print_prob_info( HSCANRESULTS hResults, int iWhichProblem )
{
    char attrib[MAX_STRING];
    int attrib_size;
    int iDisposition;

    attrib_size = MAX_STRING;
    ScanResultGetProblem( hResults,
        iWhichProblem,
        SC_PROBLEM_FILENAME,
        attrib,
        &attrib_size );
    printf( "File Name: %s\n", attrib );

    attrib_size = MAX_STRING;
    ScanResultGetProblem( hResults,
        iWhichProblem,
        SC_PROBLEM_VIRUSNAME,
        attrib,
        &attrib_size );
    printf( "Virus Name: %s\n", attrib );

    attrib_size = MAX_STRING;
    ScanResultGetProblem( hResults,
        iWhichProblem,
        SC_PROBLEM_VIRUSID,
        attrib,
        &attrib_size );
    printf( "Virus ID: %s\n", attrib );
```

```
    attrib_size = MAX_STRING;
    ScanResultGetProblem( hResults,
        iWhichProblem,
        SC_PROBLEM_DISPOSITION,
        attrib,
        &attrib_size );

    iDisposition = SC_DECODE_DISPOSITION( attrib );
    switch( iDisposition )
    {
    case SC_DISP_UNREPAIRED:
        printf( "This infection could not be repaired\n");
        break;
    case SC_DISP_REPAIRED:
        printf( "This infection was repaired\n");
        break;
    case SC_DISP_DELETED:
        printf( "The file with this infection was deleted\n");
        break;
    default:
        printf( "Unknown Disposition\n");
        break;
    }

    attrib_size = MAX_STRING;
    ScanResultGetProblem( hResults,
        iWhichProblem,
        SC_PROBLEM_DEFINITION_DATE,
        attrib,
        &attrib_size );
    printf( "Virus Definitions dated: %s\n", attrib );

    attrib_size = MAX_STRING;
    ScanResultGetProblem( hResults,
        iWhichProblem,
        SC_PROBLEM_DEFINITION_REV,
        attrib,
        &attrib_size );
    printf( "Virus Definitions Revision: %s\n", attrib );
}
```

Chapter 4

Configuring clients using ICAP 1.0

This chapter includes the following topics:

How ICAP works

The Internet Content Adaptation Protocol (ICAP) is a request/response-based protocol that lets ICAP clients pass messages to ICAP servers for processing or adaptation. The client initiates the session by sending request messages over a TCP/IP connection to a passively waiting ICAP server on a designated port. (Port 1344 is the default ICAP port.) The server then runs the service that was requested, such as antivirus scanning; performs any transformations that are necessary, such as repairing an infected file; and sends a response back to the client with any modified data.

A single transport can be used for multiple request/response pairs. Requests are matched with responses by allowing only one outstanding request on a connection at a time. Multiple connections can be used.

The Symantec AntiVirus Scan Engine supports the ICAP response modification mode (RESPMOD). In response modification mode, an ICAP client receives a data request from an origin server. The ICAP client then passes the data to an ICAP server for evaluation and post-processing.

The Symantec AntiVirus Scan Engine supports the following ICAP methods (or commands):

- OPTIONS: Lets the client obtain information from an ICAP server about available services
  See "Determining which services are supported" on page 59.
- RESPMOD: Lets the client send files to the Symantec AntiVirus Scan Engine for scanning and repair services
  See "Sending files for scanning" on page 63.

The Symantec AntiVirus Scan Engine supports the Internet-Draft specification for ICAP 1.0 that is dated December 2001. For more information about ICAP specifications, visit the ICAP Web site at:
www.i-cap.org

About ICAP messages

ICAP clients and servers communicate through messages, which are similar in format to HTTP. ICAP messages consist of client requests and server responses. All ICAP messages consist of a start line, which includes a client request or server response (depending on the type of message), header fields, and the message body. A blank line must precede the message body to distinguish the headers from the message body.

Multiple messages can be encapsulated in a single ICAP message for vectoring of requests, responses, and request/response pairs on an ICAP server. Encapsulated messages must include an Encapsulated header, which offsets the start of each encapsulated section from the start of the message body.

See "About encapsulated messages" on page 57.

Although request and response messages have unique headers, some headers are common to both requests and responses. Table 4-1 lists the general request/response headers that the Symantec AntiVirus Scan Engine uses.

Table 4-1 General request/response headers

Header	Description
Connection	Specifies options that the message sender wants to use only for that connection and not for proxies over other connections For example: Connection: close
Date	Provides the date and time that the message was created, using standard HTTP date and time format For example: Date: Tue, 5 Nov 2002 14:29:31 GMT

About request messages

All ICAP client requests start with a request line that includes the following components:

- Method: ICAP command or operation to perform (for example, RESPMOD)
- Uniform Resource Identifier (URI): Complete host name of the ICAP server and the path of the resource that is being requested
- ICAP version: Version string for the current version of ICAP using the format ICAP/version number (for example ICAP/1.0)

The URI consists of the following components:

ICAP_URI = Scheme ":" Net_Path ["?" Query]

Scheme = "icap"

Net_Path = "//" Authority [Abs_Path]

Authority = [userinfo "@"] host [":" port]

Header fields follow the request line and specify the ICAP resource that is being requested and other information, such as cache control information. ICAP-specific headers are encapsulated. The header fields end with a blank line followed by the message body. The message body contains the encapsulated HTTP messages that are being sent for scanning and modification.

Table 4-2 lists the specific request headers that are allowed in ICAP requests.

Table 4-2 Request headers

Header	Description
Allow	Lists the methods that the resource supports. For example, a client request can include an Allow: 204 header, which indicates that it will allow the server to reply to the message with a 204 No Content response if the file does not need modification. The client must buffer the message.
From	Provides the Internet email address for the user who is sending the client request. The address should use standard HTTP mailbox format. For example: From: username@symantec.com
Host	Specifies the host name and port number of the resource being requested.
Referer	Specifies the path that the client followed to obtain the URI. This optional header lets the server generate lists of back-links to resources and trace invalid links.
User-Agent	Identifies the software program that is used by the client that originated the request. This information is used for statistical purposes, to trace protocol violations, and to tailor responses to the software capabilities.
Preview	(ICAP-specific header) Lets the client send a portion of a file to the Symantec AntiVirus Scan Engine for scanning. The client uses this header to specify the amount of data, in bytes, that will be sent for preview.

About response messages

ICAP client responses start with a status line, which includes the ICAP version and a status code. For example:

ICAP/1.0 200 OK

Status codes vary depending on the type of request.

See Table 4-3 and Table 4-6 for more information about status codes.

The status line is followed by one or more response headers that let the server pass additional information to the client that cannot be placed in the status line.

See "About RESPMOD response headers" on page 68.

About encapsulated messages

The ICAP encapsulation model provides a lightweight means of packaging multiple HTTP message sections into a single ICAP message for vectoring of requests, responses, and request/response pairs on an ICAP server. An encapsulated section can consist of either HTTP message headers or bodies.

Encapsulated message bodies must be transferred using chunked transfer coding. This keeps the transport-layer connection between the client and server open for later use and lets the server send incremental responses to reduce the latency that is perceived by users. Encapsulated headers are not chunked. This lets the ICAP client copy the header directly from the HTTP client to the ICAP server without having to reprocess it.

The encapsulated header must be included in every ICAP message, except for OPTIONS requests. This header provides information about where each encapsulated section and message body starts and ends.

For example:

Encapsulated: req-hdr=0, res-hdr=45, res-body=100

This example indicates that the message encapsulates a group of request headers, response headers, and a response body at 0, 45, and 100 byte offsets. Byte offsets use a decimal format; however, chunk sizes within an encapsulated body use a hexadecimal format. If none of the message body is encapsulated, a null-body header is used.

Encapsulated headers use the following syntax:

encapsulated_header: "Encapsulated: " encapsulated_list

encapsulated_list: encapsulated_entity |

encapsulated_entity ", " encapsulated_list

encapsulated_entity: reqhdr | reshdr | reqbody | resbody | optbody

reqhdr = "req-hdr" "=" (decimal integer)

reshdr = "res-hdr" "=" (decimal integer)

reqbody = { "req-body" | "null-body" } "=" (decimal integer)

resbody = { "res-body" | "null-body" } "=" (decimal integer)

optbody = { "opt-body" | "null-body" } "=" (decimal integer)

Encapsulated headers must end with a blank line to make them readable and to terminate line-by-line HTTP parsers.

About the antivirus scanning process

The Symantec AntiVirus Scan Engine provides basic antivirus scanning services to ICAP clients through the RESPMOD method.

The general process is as follows:

- A client application receives a request to access data.
- The client application forwards the data (or a portion of it for preview) to the Symantec AntiVirus Scan Engine for scanning using the RESPMOD method.
  See "Sending files for scanning" on page 63.
- The Symantec AntiVirus Scan Engine processes the request, performs any transformations that are necessary (such as repairing infected files), and sends a response back to the client with any modified data.

Before sending files, the client can query the ICAP server using the OPTIONS method to determine which services are supported.

See "Determining which services are supported" on page 59.

Determining which services are supported

The OPTIONS method lets a client application query an ICAP server for information about supported services and commands and preferred file handling methods. The client application should perform this query before sending files for scanning.

The OPTIONS method consists of a request line that contains the address or name of the server on which the Symantec AntiVirus Scan Engine is installed and the URI for the Symantec AntiVirus Scan Engine service that you want to query.

When the Symantec AntiVirus Scan Engine receives an options request from a client application, it sends a response that includes the following information:

- Maximum number of simultaneous connections allowed
- Preferred data preview size
- Preferred file handling methods
- Supported methods (for example, RESPMOD)

Querying the AVSCAN service

The AVSCAN service performs scanning, repair, and delete functions using the scanning preferences that you specify through the Symantec AntiVirus Scan Engine administrative user interface.

Use the following format to specify the URI:

icap://<Server>/avscan

The following is a sample OPTIONS request.

```
----- Begin OPTIONS Request -----
OPTIONS icap://saves.com/avscan ICAP/1.0
Host: icapclient.savese.com
----- End OPTIONS Request -----
```

The AVSCAN service returns a response, which includes a status line followed by a series of response headers. The following is a sample OPTIONS response.

```
----- Begin OPTIONS Response -----
ICAP/1.0 200 OK
Date: Sun Jul 7 22:31:00 2002
Server: Symantec AntiVirus Scan Engine/4.0.0.0
ISTag: "123…"
Methods: RESPMOD
Allow: 204
Preview: 4
Transfer-Complete: exe,com,dll,doc,xls,…
Transfer-Preview: *
Max-Connections: 32
Options-TTL: 3600
Encapsulated: null-body=0
----- End OPTIONS Response -----
```

This response informs the client that, besides the OPTIONS method, the only supported method is RESPMOD, that the optional 204 shortcut is supported, that four bytes of preview information are preferred, that common executable files should always be sent in their entirety and everything else should be sent for preview, and that the data in this response may be cached up to one hour. The maximum number of simultaneous connections that the Symantec AntiVirus Scan Engine supports may vary, depending on the operating environment. In this example, the server supports a maximum of 32 simultaneous connections.

See "OPTIONS response codes" on page 61 and "OPTIONS response headers" on page 61.

OPTIONS response codes

Table 4-3 lists the possible response codes to an OPTIONS request.

Table 4-3 OPTIONS response codes

Response code	Text	Description
200	OK	Server processed request successfully
400	Bad request	Syntax error or other problem parsing the request
404	Not found	URI in request does not correspond to an available service
405	Method not implemented	Not valid unless OPTIONS is misspelled
408	Request timeout	Client took too long to send request
500	Internal server error	Generic problem with server
503	Service unavailable/ overloaded	Server not ready to provide service
505	ICAP version not supported	Only ICAP 1.0 is supported with this method
551	Resource unavailable	Memory or disk problem on server

OPTIONS response headers

Table 4-4 lists the response headers that are included in an OPTIONS response.

Table 4-4 OPTIONS response headers

Header	Description
Date	Specifies the date and time, as set on the server clock.
Server	Specifies the name and version number of the ICAP server.

Table 4-4 OPTIONS response headers

Header	Description
ISTag	(ICAP service tag) Lets an ICAP server send service-specific information to an ICAP client. This data can be used to validate whether a server response, including cached data, is still valid. The Symantec AntiVirus Scan Engine returns an ISTag with every response to indicate the time of the most recent change. Cached data that does not match the current ISTag is no longer valid. The value is an integer that represents the number of seconds since the UNIX epoch. For example: ISTag: “99293223881”
Methods	Specifies the methods (or commands) that are supported by the service that you queried.
Allow	Lists the optional ICAP features that the server supports.
Preview	Indicates the number of bytes of data that can be sent to the Symantec AntiVirus Scan Engine for preview.
Transfer-Preview	Lists the file extensions that should be sent to the Symantec AntiVirus Scan Engine for preview before sending the entire file. An asterisk (*) wildcard character represents the default behavior for all file extensions that are not specified in another Transfer type header.
Transfer-Complete	Lists the file extensions that should always be sent in their entirety to the Symantec AntiVirus Scan Engine and that should not be previewed. An asterisk (*) wildcard character represents the default behavior for all file extensions that are not specified in another Transfer type header.
Max-Connections	Indicates the maximum number of simultaneous ICAP connections that the server supports.
Options-TTL	Indicates the time (in seconds) during which the response is valid or cached. A blank header indicates that the response does not expire.
Encapsulated	Offsets the start of each encapsulated section from the start of the message body.

Sending files for scanning

The Symantec AntiVirus Scan Engine supports one URI for scanning and repair services, which uses the following format:

icap://server.name:port/avscan

Replace server.name with the name of the server on which the Symantec AntiVirus Scan Engine is running. The port number is optional if the Symantec AntiVirus Scan Engine is running on port 1344, which is the default ICAP port.

Sending portions of files for preview

The Symantec AntiVirus Scan Engine can preview data to determine whether it needs to be scanned based on known virus behavior. For example, .gif files are typically not scanned because they generally do not contain executable code. The rules for which types of files are suitable for preview are determined by the inclusion and exclusion lists that are configured in the Symantec AntiVirus Scan Engine.

Before a file is sent for scanning, the client should send an OPTIONS request to determine whether a file type is suitable for preview and how much data should be sent. The Symantec AntiVirus Scan Engine provides this information in the following headers of the OPTIONS response message:

- Preview: Indicates the preferred number of bytes of data that can be sent
- Transfer-Complete: Indicates which file types should be sent in their entirety
- Transfer-Preview: Indicates which file types should be sent for preview

See Table 4-4 for more information about OPTIONS response headers.

Table 4-5 details the scanning behavior based on the scanning policies that are configured in the Symantec AntiVirus Scan Engine.

For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

Table 4-5 Scanning behavior

Scanning policy	Transfer-Complete header	Transfer-Preview header	Scan behavior
Scan all files regardless of extension	Asterisk (*) character	Not used	The Symantec AntiVirus Scan Engine scans every file in its entirety without previewing it first.
Scan files with the following extensions (inclusion list)	List of file extensions	Asterisk (*) character	The Symantec AntiVirus Scan Engine scans the entire file for each file type that is in the inclusion list. Other file types are previewed for dangerous content.
Scan all files except those with the following extensions (exclusion list)	Asterisk (*) character	List of file extensions	The Symantec AntiVirus Scan Engine previews the file types that are listed in the Transfer-Preview header for dangerous content. All other file types, including unidentified file types, are scanned in their entirety.

If an OPTIONS response indicates that a file is suitable for preview, the client should include a Preview header in the request message that indicates the portion of data, in bytes, that is being sent for preview. The Symantec AntiVirus Scan Engine then evaluates the initial chunk of data to determine whether a full scan is required. If so, the Symantec AntiVirus Scan Engine requests the remainder of the data. Scan results are returned in the RESPMOD response message.

See "Interpreting RESPMOD response messages" on page 65.

Allowing no content responses

The Allow:204 header is an optional header that lets the Symantec AntiVirus Scan Engine return a 204 No Content response code if the message does not require modification. This can optimize server performance because the Symantec AntiVirus Scan Engine can declare a file clean without waiting to receive the entire message and does not have to return the message. The processing burden is placed on the client, which must buffer the entire message during the scan. The Symantec AntiVirus Scan Engine returns a 204 No Content response outside of a preview only if the client request includes an Allow: 204 header.

Interpreting RESPMOD response messages

After performing a scan, the Symantec AntiVirus Scan Engine returns a response message, which indicates the scan results and, if applicable, any modified data. Response messages start with an ICAP status line, which includes the ICAP version and a status code. For example:

ICAP/1.0 200 OK

The status line is followed by one or more response headers that let the server pass additional information to the client that cannot be placed in the status line. If no virus is detected, the Symantec AntiVirus Scan Engine also returns a copy of the scanned data to the client, unless the client request includes an Allow: 204 header. If so, the Symantec AntiVirus Scan Engine only returns a response message. If a virus is detected, the scan policy settings determine whether the Symantec AntiVirus Scan Engine attempts to repair the file and whether modified content is returned to the client.

The following example shows a standard RESPMOD request:

```
----- Begin Standard RESPMOD Request -----
RESPMOD icap://saves.com/avscan ICAP/1.0
Host: icapclient.savese.com
Allow: 204
Preview: 4
Encapsulated: req-hdr=x res-hdr=y res-body=z
[ Request headers…]
[ Response headers…]
4
[ First four bytes of body data… ]
0;
----- End Standard RESPMOD Request -----
```

RESPMOD response codes

Response codes in the 200 class indicate whether a virus was found and which action, if any, was taken to repair the file. Response codes in the 400 and 500 classes are error codes. Table 4-6, Table 4-7, and Table 4-8 list the possible response codes to a RESPMOD scanning request.

Table 4-6 RESPMOD response codes for successfully processed scanning

Response code	Text	Description
100	Continue	The Symantec AntiVirus Scan Engine completed a preview and requires additional data.
200	OK	The request was processed successfully. In its default configuration, the Symantec AntiVirus Scan Engine returns a 200 response if no virus was detected or if a virus was detected but either the file cannot be repaired or the scan engine is configured for scan only mode. If the Symantec AntiVirus Scan Engine is configured to send an ICAP 403 response, the Symantec AntiVirus Scan Engine returns a 200 response only if no virus was detected. See "Changing an ICAP response" on page 21.
201	Created	A virus was detected and the file has been repaired (not valid for scan only mode). The response also includes the repaired data.
204	No content necessary	No virus was detected and the client sent an Allow:204 header, which indicates that the Symantec AntiVirus Scan Engine does not need to return data to the client.

Table 4-7 Client error RESPMOD response codes

Response code	Text	Description
400	Bad request	The Symantec AntiVirus Scan Engine was unable to process the request because of a syntax error or other general problem in the client request.

Table 4-7 Client error RESPMOD response codes

Response code	Text	Description
403	Forbidden. Infected and not repaired.	The data was infected and cannot be repaired or the Symantec AntiVirus Scan Engine is configured for scan only mode. **Note:** This response is the standard ICAP behavior, as documented in the ICAP 1.0 draft specification. However, to support NetApp NetCache clients, the Symantec AntiVirus Scan Engine does not follow this behavior by default. If your client application closely follows the ICAP 1.0 draft standard, you might need to change the default setting for an ICAP response. See "Changing an ICAP response" on page 21.
404	Not found	The URI that was specified in the client request does not match any service that is available on the server.
405	Method not implemented	The client requested a method that is not supported by the server (other than OPTIONS or RESPMOD). The response also includes an Allow header line that identifies the supported methods.
408	Request timeout	The client took too long to send the request.

Table 4-8 Server error RESPMOD response codes

Response code	Text	Description
500	Internal server error	A generic problem occurred on the server.
503	Service unavailable/ overloaded	The server is not ready to provide service.
505	ICAP version not supported	The ICAP client is using a version of ICAP other than 1.0.
533	Error scanning file	An error occurred during file scanning that prevented the Symantec AntiVirus Scan Engine from completing the scan.

Table 4-8 Server error RESPMOD response codes

Response code	Text	Description
539	Aborted - No AV scanning license	The Symantec AntiVirus Scan Engine is unable to scan the data because a valid license does not exist. See "About licensing" on page 10.
551	Resource unavailable	A memory or disk problem occurred on the server.

About RESPMOD response headers

Table 4-9 lists the RESPMOD response headers that are specific to antivirus scanning.

Table 4-9 RESPMOD response headers

Header	Description
Server	Provides information about the software that is used by the origin server to handle the request. If the request is handled by a proxy server, the proxy server can add information using the Via field, but cannot modify the server response.
ISTag	(ICAP service tag) Lets an ICAP server send service-specific information to an ICAP client. This data can be used to validate whether a server response, including cached data, is still valid. The Symantec AntiVirus Scan Engine returns an ISTag with every response to indicate the time of the most recent change. Cached data that does not match the current ISTag is no longer valid. The value is an integer that represents the number of seconds since the UNIX epoch. For example: ISTag: "99293223881"
X-Outer-Container-Is-Mime	(Optional header) Indicates whether the outer container is a valid MIME container. A client application can use this information to reject content that does not meet this criteria.

Table 4-9 RESPMOD response headers

Header	Description
X-VIOLATIONS-FOUND	Indicates the number of infections or threats that were found in the scanned data. This header is always returned. If no virus was detected, a zero (0) count is returned. If a virus was detected, the X-VIOLATIONS-FOUND header specifies the number of violations that were found. The header is followed by a series of indented lines that provide the following information: ■ File name: The name of the scanned file or the name of a nested component within the scanned file, with each component name separated by a slash mark (/). ■ Virus name: The English-readable name of the virus. ■ Virus ID: A numeric code for the virus. ■ Disposition: An integer value that indicates what action was taken to fix the file. Zero (0) indicates that the file is unrepairable, one (1) indicates that the file was repaired, and two (2) indicates that the file was deleted.

Sample response

The following example shows an error response that indicates that the Symantec AntiVirus Scan Engine is unable to process the request.

```
---------- BEGIN respmod response (ERROR) ----------
ICAP/1.0 400 Bad Request
Date: Mon Apr 15 22:27:53 2002
Server: Symantec_AntiVirus_Scan_Engine/4.0.0.0
Connection: keep-alive
ISTag: "F01CD83457"
X-SAVSE-AV-Status: 0291<FS>9032
Encapsulated: null-body=0
---------- END   respmod response (ERROR) ----------
```

Appendix A

Native protocol reference

This chapter includes the following topics:

Native protocol basics

The Symantec AntiVirus Scan Engine native protocol is a request/reply-based protocol. The protocol version, the request, and the file are all transmitted by the client upon connection with the scan engine. The reply consists of a reply code, scan results, and the file if the file has been modified (the client knows this from the reply code).

The information in this chapter is intended for informational or debugging purposes only. Use the client-side application program interface (API) C library to implement custom integrations using the native protocol.

Definition of a client send

Use the client send when actual files are passed to the Symantec AntiVirus Scan Engine via a socket over the network when the Symantec AntiVirus Scan Engine is running on a separate computer.

Note: All file names must be Unicode UTF-8 encoded.

```
Version 2<CRLF>
<socket-command><CRLF>
<filename><CRLF>
<filesize><CRLF>
<filesize-bytes-of-data>
```

Definition of <socket-command>

Use one of the following commands to indicate the function that the Symantec AntiVirus Scan Engine should perform on files to be scanned:

- AVSCAN: Scan only; no repair.
- AVSCANREPAIR: Scan and repair if possible.
- AVSCANREPAIRDELETE: Scan and repair; delete if repair is not possible.

Definition of a local scan request

For cases in which the client application can pass the file name to the Symantec AntiVirus Scan Engine, use a local scan request to let the Symantec AntiVirus Scan Engine open the file and scan it in place.

Note: All file names must be Unicode UTF-8 encoded.

```
Version 2<CRLF>
<local-command><CRLF>
<filename><CRLF>
```

Definition of <local-command>

Use one of the following commands to indicate the function that the Symantec AntiVirus Scan Engine should perform on local files to be scanned:

- AVSCANLOCAL: Local file version of AVSCAN
- AVSCANREPAIRLOCAL: Local file version of AVSCANREPAIR
- AVSCANREPAIRDELETELOCAL: Local file version of AVSCANREPAIRDELETE

Definition of a server reply

If there is an error, a reply code is returned and the connection is closed (after the <CRLF>).

```
Reply-Code<CRLF>
<scan-results>
<receive-file>
```

Note: If the Symantec AntiVirus Scan Engine crashes or a network error occurs, a socket connection can be dropped without the client side of the connection being notified. Clients should be implemented using blocking sockets. Clients should interpret a 0-byte socket recv() return value as a closed connection.

Reply-code syntax

The syntax for a reply is as follows:

```
<3-digit-reply-code> <SP> <line-of-text> <CRLF> <optional-data>
```

Reply codes are based on the syntax shown in Table A-1.

Table A-1 Reply-code syntax

Syntax	Description
1yz	Positive Preliminary reply
2yz	Positive Completion reply
3yz	Positive Intermediate reply
4yz	Transient Negative Completion reply
5yz	Permanent Negative Completion reply
x0z	Syntax
x1z	Information
x2z	Connections
x3z	File Scan

For example, 22z indicates the positive completion of a connection command.

Native protocol reply codes

Table A-2 lists the reply codes that are generated for the native protocol.

Table A-2 Native protocol reply codes

Reply code	Description
200	Command okay.
201	Output file available.
203	Local output file available.
220	Symantec AntiVirus Scan Engine ready.
221	Service closing transmission channel.
230	File scanned.

Table A-2 Native protocol reply codes

Reply code	Description
420	Service not available, closing transmission channel.
430	File not acceptable at this time.
500	Syntax error, command unrecognized.
501	Syntax error in parameters.
502	Command not implemented.
503	Bad sequence of commands.
504	Unsupported protocol version.
530	File not acceptable.
531	File unscannable.
532	Output file unavailable.
533	Error scanning file.
534	File name exceeds configured length.
535	Maximum Extract Time exceeded - scan incomplete.
536	Maximum Extract Depth exceeded - scan incomplete.
537	Maximum Extract Size exceeded - scan incomplete.
538	Malformed container file found. File not scanned.
539	Aborted - No AV scanning license.

Initial reply

When the connection is first established, an initial reply is made before the first command. The reply is one of the following:

- 220 Symantec AntiVirus Scan Engine ready. <CRLF> <protocol-version-number> <CRLF>
- 420 Service not available, closing transmission channel. <CRLF>

Definition of <receive-file>

The syntax for <receive-file> is as follows:

- 201 Output file available. <CRLF> <filesize> <CRLF> <filesize-bytes-of-data>
- 203 Local output file available. <CRLF> <filename> <CRLF>
- 420 Service not available, closing transmission channel. <CRLF>
- 532 Output file unavailable. <CRLF>

Definition of <scan-results>

The syntax for <scan-results> is as follows:

```
<scan-status> <CRLF>
<definitions-date> <CRLF>
<definitions-version> <CRLF>
<infection-count> <CRLF>
<infection-info>
<infection-info>
...
<infection-info>
```

There are <infection-count> instances of <infection-info>. The <infection-count> may be zero.

<scan-status>

<scan-status> is an integer value that can be any of the values that are listed in Table A-3.

Table A-3 Integer values for <scan-status>

Value	Definition
0	File clean
1	File infected, not repaired
2	File infected, partially repaired
3	File infected, fully repaired

<definitions-date>

The syntax for <definitions-date> is as follows:

<YYYYMMDD>

<definitions-version>

The <definitions-version> is an integer that is greater than or equal to 1.

<infection-info>

The syntax for <infection-info> is as follows:

```
<filename> <CRLF> <virusname> <CRLF> <virusID> <CRLF> <disposition>
<CRLF>
```

A <filename> is the name of the scanned file or the name of a nested component within the scanned file, with each component name separated by a / character. For example, if the scanned file is Badfile.zip, a subcomponent name might be Badfile.zip/Message.mme/Attachment.exe. File names may contain embedded spaces.

A <virusname> is the English-readable name of the virus, <virusID> is a numeric code for the virus, and <disposition> is an integer value. The possible values for <disposition> are listed in Table A-4.

Table A-4 Integer values for <disposition>

Value	Definition
0	Unrepaired
1	Repaired
2	Deleted

Scenarios

Scan of a clean file

R: 220 Symantec AntiVirus Scan Engine ready.
R: 2// protocol version number
S: Version 2// Client version number
S: AVSCANREPAIR// Command
S: WINWORD.EXE// file name
S: 1111// file size
S: <1111 bytes of data>// file data
R: 230 File scanned.// Reply code
R: 0// file clean
R: 20000214// defs date
R: 1// defs version
R: 0// infection count
R: 532 Output file unavailable// Reply code

Scan of a file with one virus

R: 220 Symantec AntiVirus Scan Engine ready.
R: 2// protocol version number
S: Version 2// Client version number
S: AVSCANREPAIR// Command
S: INFECTED.EXE// file name
S: 11706// file size
S: <11706 bytes of data>// file data
R: 230 File scanned. // Reply code
R: 3// infected, repaired
R: 20000214// defs date
R: 1// defs version
R: 1// infection count
R: INFECTED.EXE// component name
R: Cascade// virus name
R: 226// virus id
R: 1// component status (repaired)
R: 201 Output file available// Reply code
R: 10000// File size of repaired file
R: <10000 bytes of data>// Repaired file data

Repair of a file with one repairable and one unrepairable virus

R: 220 Symantec AntiVirus Scan Engine ready.
R: 2// protocol version number
S: Version 2// Client version number
S: AVSCANREPAIR// Command
S: BADFILE.ZIP// file name
S: 33333// file size
S: <33333 bytes of data>// file data
R: 230 File scanned.// Reply code
R: 2// partially repaired
R: 20000214// defs date
R: 1// defs version
R: 2// infection count
R: BADFILE.ZIP/BADSUBFILE.EXE// component name
R: Cascade// virus name
R: 226// virus id
R: 1// (repaired)
R: BADFILE.ZIP/badsubcontainer.zip/BadSubFile2.exe
// component name
R: DirAct// virus name
R: 3434// virus id
R: 0// (unrepaired)
R: 532 Output file available// Reply code
R: 30000// File size of repaired file
R: <30000 bytes of data>// Repaired file data

Scan only of a file local to the server

R: 220 Symantec AntiVirus Scan Engine ready.
R: 2// Protocol version number
S: Version 2// Client version number
S: AVSCANLOCAL// Command
S: /tmp/eicar68.com// file name (on server)
R: 230 File scanned.// Reply code
R: 1// infected, not repaired
R: 20001031// defs date
R: 5// defs version
R: 1// infection count
R: /tmp/eicar68.com// file name
R: EICAR Test String.68// virus name
R: 6496// virus id
R: 0// (unrepaired)
R: 532 Output file unavailable.// Reply code

Scan and repair of a file local to the server

R: 220 Symantec AntiVirus Scan Engine ready.
R: 2// Protocol version number
R: Version 2// Client version number
S: AVScanRepairDeleteLocal// Command
S: \work\test.exe// file name (on server)
R: 230 File scanned.// Reply code
R: 3// repaired
R: 20001208// defs date
R: 17// defs version
R: 1// infection count
R: \work\test.exe// file name
R: EICAR Test String.68// virus name
R: 6496// virus id
R: 1// (repaired)
R: 203 Local output file available.// Reply code
R: \work\test.exe// Path to repaired file

Index

H

I

L

M

N

O

P

R

S

U

V

W